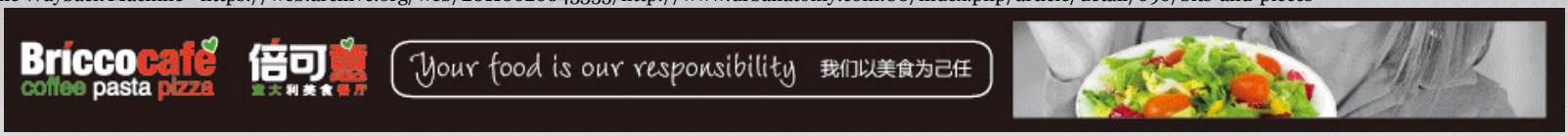
The Wayback Machine - https://web.archive.org/web/20110626045355/http://www.urbanatomy.com:80/index.php/article/detail/696/bits-and-pieces



Bits and Pieces

by nickland @ Thursday, 23 June 2011 16:00

P2P or not 2P, that is the question

As the US dollar reaches depths of debasement that would have stretched the imagination of Caligula, people have been searching for alternative candidates for a global reserve currency. The problem is formidable. The Euro and Japanese Yen face comparable calamities of their own (mixing debt crisis and demographic collapse), the Chinese Yuan is non-convertible, and the IMF's hybrid Special Drawing Rights (SDRs) merely bundle together a group of troubled fiat currencies under a technocratic acronym.

Precious metals enthusiasts have an obvious option, and one that is already being spontaneously exercised. Yet whilst growing numbers will no doubt cling to gold and silver as financial lifeboats, their wider use as currency (as opposed to stores of value) is obstructed by an intimidating range of technical and political problems. They are not digitally transferable without complicated mediating instruments, and they remain exposed to extreme political risk – financial crises have been regularly accompanied by seizures and controls directed at private precious metals holdings and transactions.

To overcome such problems, a currency would need to be structurally immunized against the depredations of central bankers, to share the deflationary bias of precious metals, and to participate fully in the technical trend towards mathematical abstraction and electronic communicability, whilst also enjoying strong cryptographic protection against surveillance, expropriation, and fraud. Astonishingly, such a currency seems already to exist. Its name is 'Bitcoin'.

The twin, interactive drivers of modernity – commerce and technology – come together in Bitcoin with unprecedented fusional intensity. This is a currency that is simultaneously an open source computer program, entirely native to cyberspace, and a financial innovation, conducting a real-time experiment that is at once social, technical, and economic. Built on the foundations of public key encryption (PKE), it creates a peer-to-peer open network – without any controlling node or discretionary human management – to sustain a radically decentralized monetary system.

Originally devised by Satoshi Nakamoto (whose outline paper can be found here), Bitcoin disconnects trust from authority. In particular, it is designed to overcome the problem of double spending.

ADVERTISEMENT

Video

Brawl on the Bund is back!

Brawl on the Bund is back!

ADVERTISEMENT

Latest Podcasts

1. Hello Long Weekend! The That's
2. We give you Fever! The That's
3. Champion of the World! The That's
4. We're Back! The That's Shanghai

Because digital 'goods' can be replicated at near-zero cost, they are economically defined as 'non-r computer, I now own it, and you do not. As with all rivalrous goods, ownership implies exclusion. I program, on the other hand, there is no reason to assume that you have not kept a copy for yourse could not be sold to multiple purchasers. Such non-rivalrous goods pose numerous intriguing econ is entirely clear: non-rivalrous money is an impossibility. Without scarcity, or exclusive exchange, t quantity loses all sense, as does monetary value, spending and investment, and consumer choice.

The Bitcoin algorithm makes a digital currency rivalrous, and thus effective as money, without reco authority. It does so by initiating an automatic or spontaneous ecology, in which computers on the exchanges as a side-effect of 'mining' for new coins. Nodes earn new coins, at a diminishing rate, b puzzle – accessible only to a brute force, computationally-intensive approach – and thus exhibiting p the system from malicious interventions, by establishing a practically insurmountable barrier to any record of exchanges. Competent discussions can be found here, here, and (most diversely) here.

This problem, and solution, is very far from arbitrary. It is precisely because existing fiat currencies non-rivalrous characteristics that alarm about currency debasement has reached such a pitch of exa bank, in the course of running a typically loose monetary policy, can simply speed up the printing p electronic equivalent, the integrity of the money supply is devastated at the root. Bitcoin rigorously discretion from its system, by instantiating a theory of sound money as a precisely and publicly def

Unsurprisingly, the Bitcoin monetary aggregate is modeled on precious metal, generated by miners with rising extraction costs. The reward for coin mining falls over time at a logarithmic (Zenonian) r fractionally under 21,000,000 BTC. Each Bitcoin can be subdivided to eight decimal places, to a tot (2,100,000,000,000,000) fragments, equivalent to 210,000 Bitcoin 'quanta' for each of the 10 billi earth's anticipated climax human population. A Bitcoin quantum (0.00000001 BTC) is named a 'Sat Nakamoto), although amendment to the system allowing for further sub-division at some future sta total size of the Bitcoin economy look here.)

Bitcoin is programmed for deflation (of a sort). This is a source of delight to hard money types, and loose money (inflationary) camp. As an experiment, the great merit of Bitcoin is to raise this antago reciprocal polemics, to that of potential historical evidence -- and real choice. Austrolibertarians hav money systems are biased to deflation, and that central banking encourages inflation as a surreptit expropriation, to ultimately disastrous effect. Keynesians, in contrast, deplore deflation as an econ productive investment and employment. Empirical testing could soon be possible.

Numerous other questions, theoretical and practical, present themselves. At the practical level, such out through speculative volatility, institutional adaptations, and technical challenges. Since the enti very small, relatively modest shifts in economic behavior yield wild swings in BTC value, including b collapses, incontinent hype, and extravagant accusations. Despite the resilience of the core algorithm supporting the Bitcoin economy remain vulnerable to theft, fraud, and malicious interventions. As w experiment, the developmental trajectory of Bitcoin is likely to be tumultuous and highly unpredict

The theoretical questions can be entertained more calmly. The most important of these concern th and its future. Does Bitcoin successfully simulate the significant features of precious metals, such t discarded from the monetary equation as irrelevant dross? How powerful are the forces leading to r first-mover advantage 'lock-in' Bitcoin at the expense of later alternatives? Or will multiple money s heterogeneous ones – continue to co-exist? Is Bitcoin merely one stage in an open-ended sequence or does it capture the essential features of money quite definitively (leaving room only for incremen tinkering)?

Supporters of the monetary status quo might insist on a further, more derisive line of questioning: irrelevance, or a deluding libertarian cipherpunk fantasy, to be judged eventually as something akin that, ultimately, the largest questions will be political, and the most heated discussions already are

Can governments afford to tolerate unmanaged, autonomous currencies? We'll see.

Comments

Leave a Comment

Submit

Urbanatomy Media Products

All Rights Reserved. Urbanatomy Media - Shanghai, Beijing & Pearl River Delta. China
沪ICP备08007913号